

Emotet botnet is now heavily spreading QakBot malware

By Ionut Ilascu

Published: 2020-07-21 · Archived: 2026-04-05 14:39:01 UTC

```
7701CFA0 C5CD LDS ECX,EBP Illegal use of register C5CD
7701CFA2 FE DS DWORD PTR DS:[??] EDI Unknown command 701CFA2 FE
7701CFA3 FFE9 BYTE PTR DS:[??] FAR ECX Illegal use of register FFE9
7701CFA5 AB STOS DWORD PTR ES:[EDI] 7701CFA5 AB
7701CFA6 8402 TEST BYTE PTR DS:[EDX],BH 7701CFA6 8402
7701CFA8 00BF ADD BYTE PTR DS:[EDI],BH 7701CFA8 00BF
7701CFAE EB E9 JMP FAR ECX 7701CFAE EB E9
7701CFB0 7B 00 JPO SHORT ntddi 7701CFB0 7B 00
7701CFB2 25 00300038 AND EAX,80000000 7701CFB2 25 003
7701CFB7 006C00 78 STOS DWORD PTR ES:[EDI] 7701CFB7 006C00
7701CFBB 002D 00250030 ADD BYTE PTR DS:[EDI],BH TEST BYTE PTR DS:[EDX],A 7701CFBB 002D 0
7701CFC1 003400 X,30002500 ADD BYTE PTR DS:[EAX+EAX] ADD BYTE PTR DS:[EDI+C00 7701CFC1 003400
7701CFC4 78 00 JPO SHORT ntddi 7701CFC4 78 00
7701CFC6 2D 00250030 SUB EAX,80000000 JPO SHORT ntddi 7701CFC6 2D 002
AND EAX,80000000
ADD EAX,EAX
ADD BYTE PTR DS:[EAX+EAX]
ADD BYTE PTR DS:[300025000]
ADD BYTE PTR DS:[EAX+EAX]
```

Researchers tracking Emotet botnet noticed that the malware started to push QakBot banking trojan at an unusually high rate, replacing the longtime TrickBot payload.

Last week, Emotet came back to life after a break of more than five months. Starting yesterday, the malspam operation [briefly](#) began installing TrickBot on compromised Windows systems again.

Things changed today when researchers noticed that Emotet was dropping QakBot. A string in the malware indicates that this trojan is now the partner of choice for Emotet botnet.



Visit Advertiser website [GO TO PAGE](#)

Full distribution

A group of researchers and system administrators united under the name [Cryptolaemus](#) to fight Emotet operations, saw today that the threat actor replaced TrickBot distribution across all epochs.

An Emotet epoch is a subgroup of the botnet running on a distinct infrastructure. Currently, there are three of them, each with separate command and control servers, distribution methods, and payloads.

Speaking to BleepingComputer, Cryptolaemus said that they saw QakBot distributed all across Emotet botnet, TrickBot being completely absent.

Security researcher [Bom](#) caught a QakBot (QBot) malware sample and fed it to the Any.Run interactive analysis tool. The results are available at this [link](#). A list with the addresses for the command and control servers (C2) is [available here](#).

Additional analysis from cybercrime intelligence company [Intel 471](#) revealed that the string for identifying this QBot campaign is “partner01,” suggesting a strong connection between Emotet and these threat actors.

However, speculating on a fallout between Emotet and TrickBot is premature as the relation between the operators of these treats two is not exclusive. Cryptolaemus said that a change in the delivered payload has happened in the past and that the original duo is very likely to resume activity.

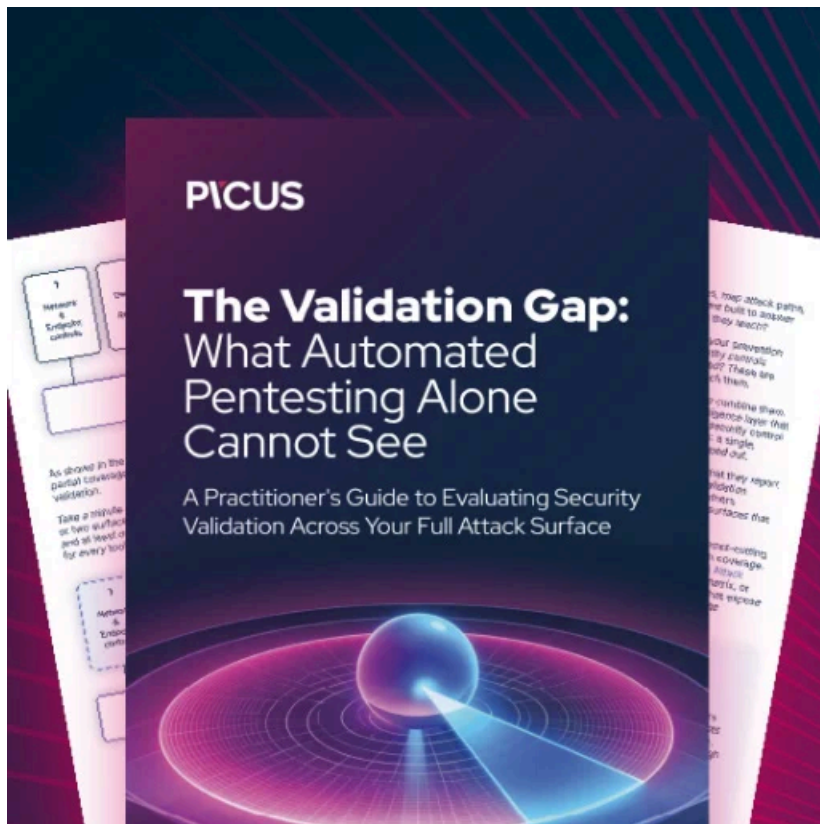
But this does not occur too often, though. For instance, Emotet was seen [delivering QakBot](#) last year.

TrickBot and QakBot are the [preferred partners](#) for Emotet. All three actors are part of the same Russian-speaking community and have been interacting for a long time.

It is unclear what QakBot drops on infected systems but [some victims may get ransomware](#) as a special delivery, ProLock in particular.

For updates on indicators of compromise and C2 addresses used in Emotet campaigns, you can follow the [Cryptolaemus Twitter profile](#).

Even if there is a different payload, Emotet still relies on emails for malware distribution, with the threat delivered via a malicious document.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/emotet-botnet-is-now-heavily-spreading-qakbot-malware/>